FUNCTIONAL SAFETY ENGINEER

CERTIFICATION COURSE

Exercise Solutions

The following slides are arranged by practical number and consist of question items followed by answer items.

Practical exercise no: 1

Fault trees

This practical exercise requires attendees to construct a fault tree diagram using the basic principles introduced in module 3.

It uses an example of a simple reactor with automatically controlled feeds that has the potential to cause a serious risk to plant personnel. Once the basic fault tree has been drawn, the model is to be adjusted to incorporate a safety-instrumented system and to demonstrate the resulting risk reduction.

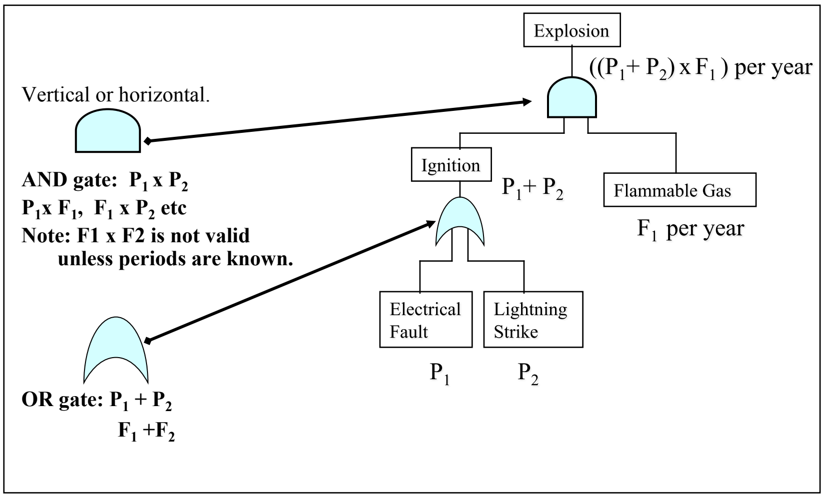
The process is a reactor with a continuous feed of fuel and oxidant. Two flow control loops are operated under a ratio controller set by the operator to provide matching flows of fuel and oxidant to the reactor.

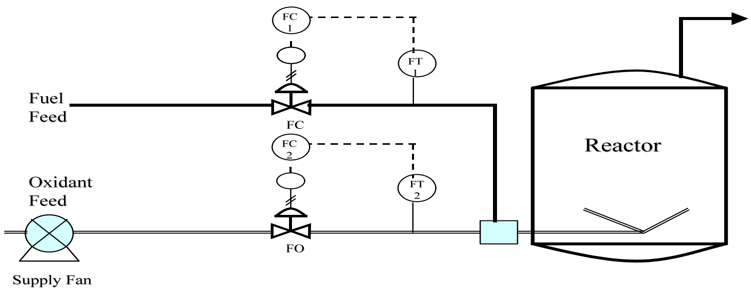
An explosive mixture can occur within the reactor if the fuel flow becomes too high relative to the oxidant flow.

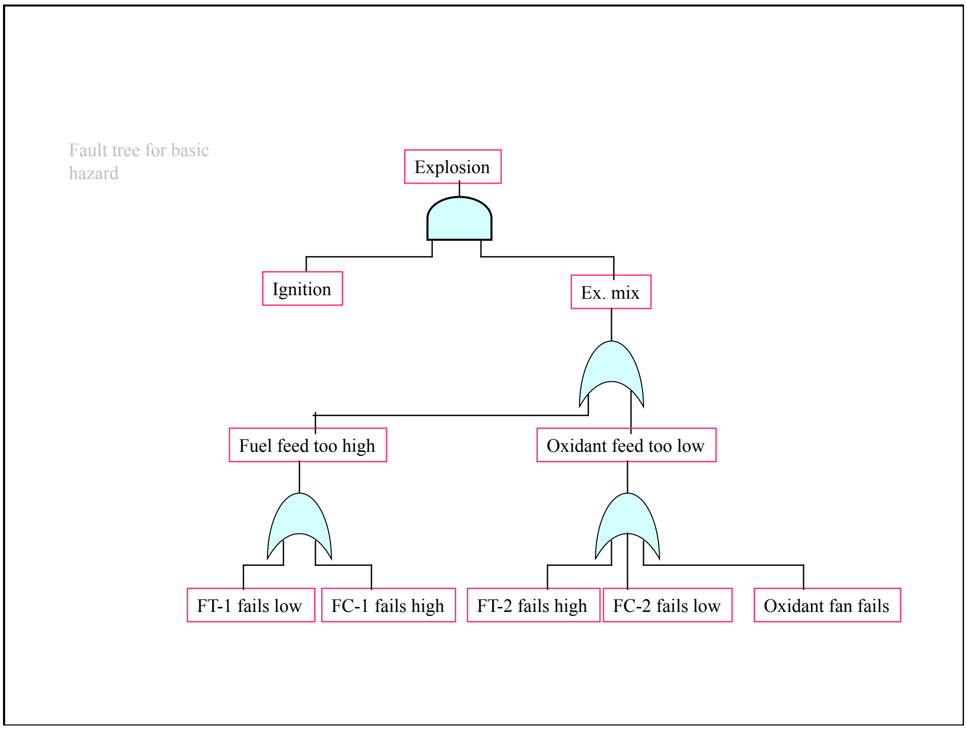
Possible causes are: Failures of the BPCS or an Operator error in manipulating the controls leading to sudden loss of oxidant feed.

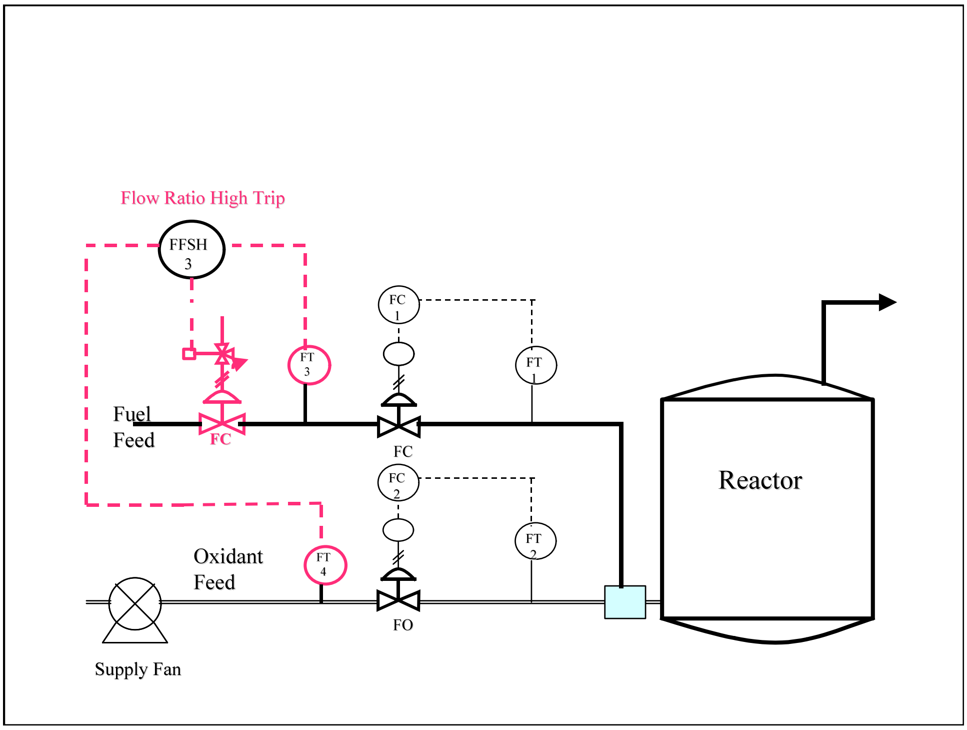
A SIS is proposed with a separate set of flow meters connected to a flow ratio measuring function that is designed to trip the process to safe condition if the fuel flow exceeds the oxidant flow by a significant amount

The tag number for this SIF is FFSH- 03

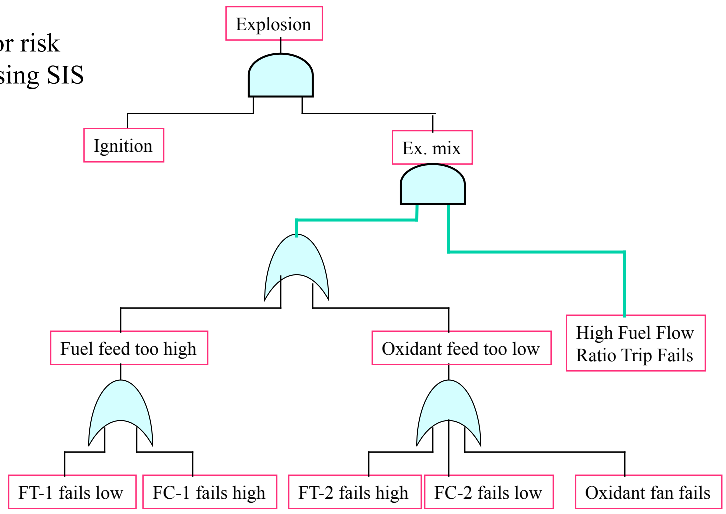

Explosion
$((P_1 + P_2) \times F_1)$ per year
Vertical or horizontal.
AND gate: $P_1 \times P_2$
$P_1 \times F_1$, $F_1 \times P_2$ etc
Note: F1 x F2 is not valid unless periods are known.
Ignition
$P_1 + P_2$
Flammable Gas
F_1 per year
Electrical Fault
Lightning Strike
P_1
P_2
OR gate: $P_1 + P_2$
$F_1 + F_2$


FC 1
FT 1
Fuel Feed
FC
FC 2
FT 2
Reactor
Oxidant Feed
FO
Supply Fan


Fault tree for basic hazard
Explosion
Ignition
Ex. mix
Fuel feed too high
Oxidant feed too low
FT-1 fails low
FC-1 fails high
FT-2 fails high
FC-2 fails low
Oxidant fan fails


Flow Ratio High Trip
FFSH 3
FT 3
FC 1
FT
Fuel Feed
FC
FC
FC 2
FT 2
Reactor
Oxidant Feed
FT 4
FO
Supply Fan

Fault tree for risk reduction using SIS



Exercise No: 2 – SIL Verification

Task 1 Calculate the single channel PFDavg and spurious trip rate for the high temperature trip example. Draw a single channel reliability block diagram and calculate using the failure rates in the table the PFDavg and the spurious trip rate for each sub system and the overall system using a proof testing interval of 6 months.

Assume the system uses 2 relays, 1 relay in the sensor subsystem and 1 relay in the logic solver subsystem, The trip actuation uses a solenoid valve and to vent the air cylinder on a valve that will drive open and release quench water into the reactor.

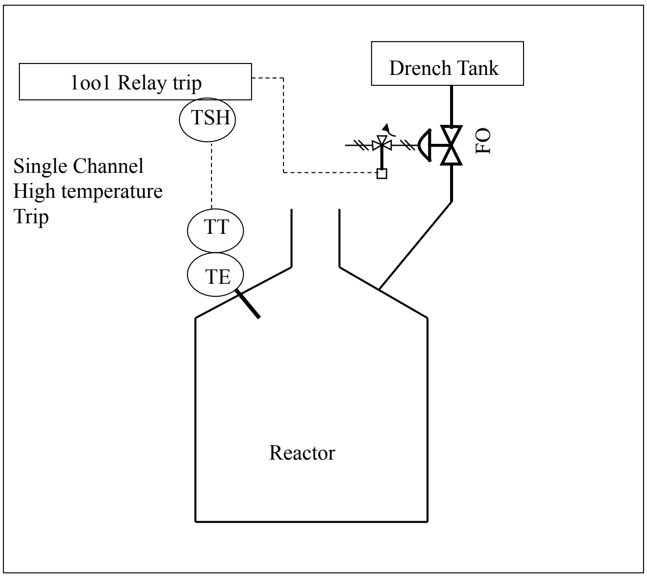
Task 2: Recalculate the PFDavg and spurious trip rate for the SIF using the second diagram showing 3 high temperature transmitters on a reactor configured 2oo3 on the basis of proof testing every 6 months, Beta Factor 10% and MTTR of 24 hours.

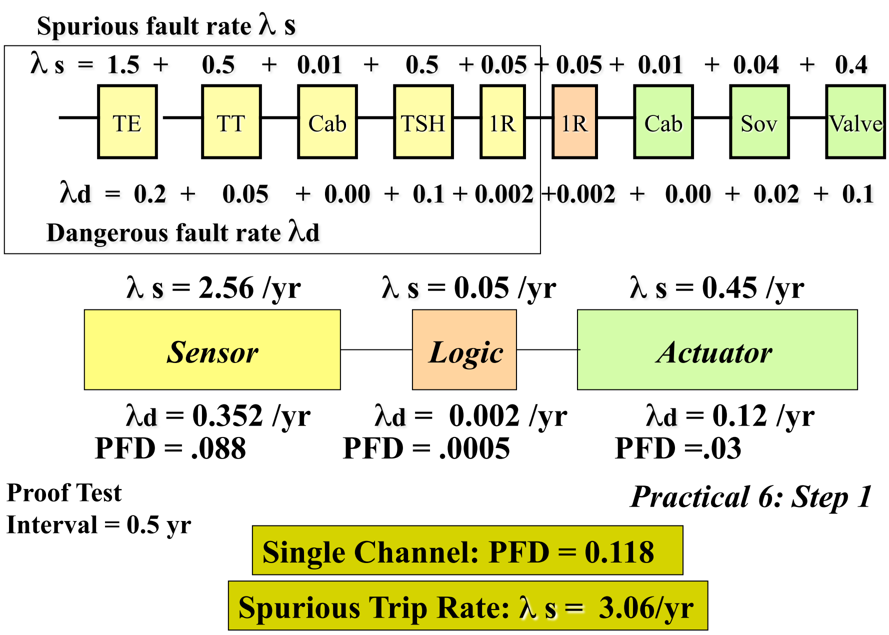
The 3 temperature transmitters each transmit to a trip amplifier device that acts as a high temperature trip device leading to a single channel actuation as in task 1

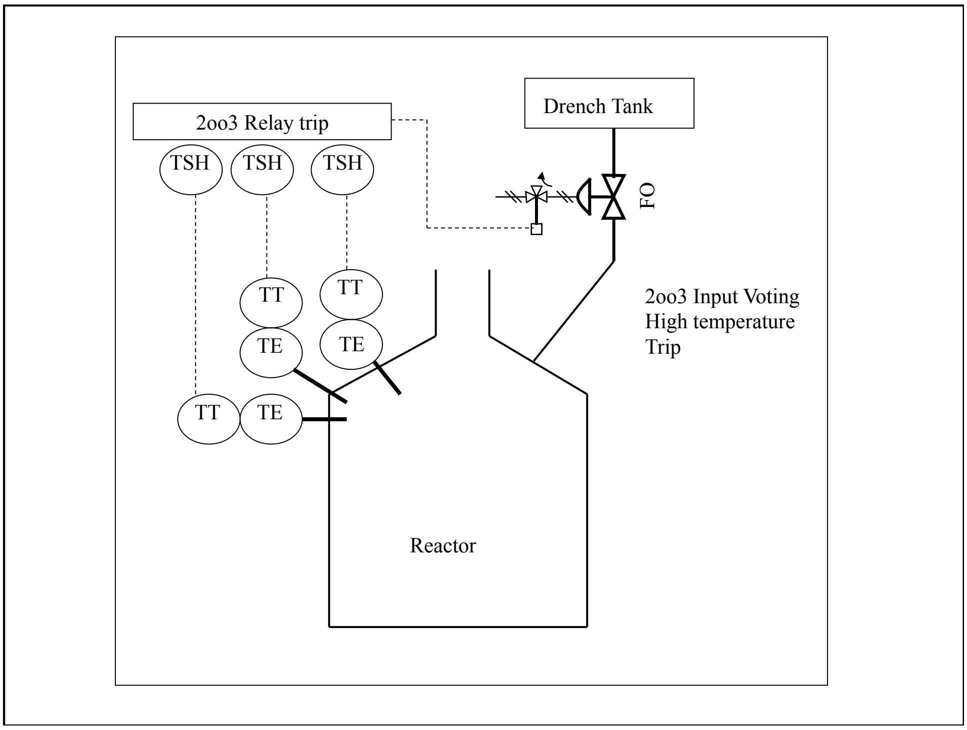
Table of fault rates for the Devices

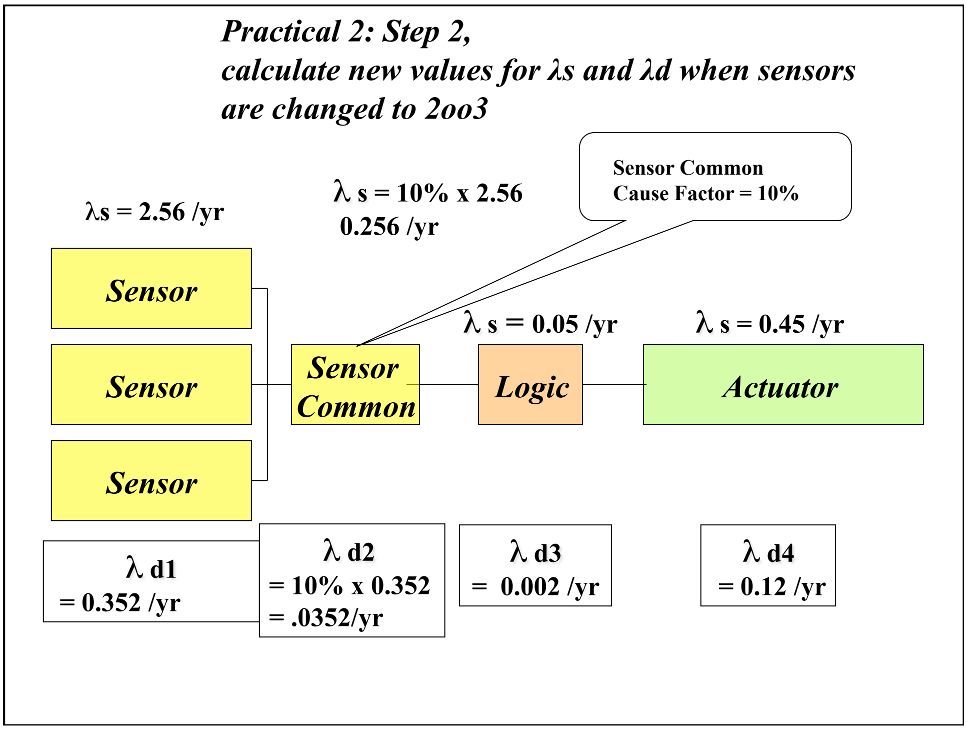
Channel Device	Fail-safe rate per year	Fail –danger rate per year
TE…element	1.5	0.20
TT .Transmitter	0.5	0.05
Cable/terminals	0.01	0.00
TSH….trip amplifier/switch	0.5	0.1
Relay (each)	0.05	0.002
Solenoid Valve	0.04	0.02
Trip Valve	0.4	0.1

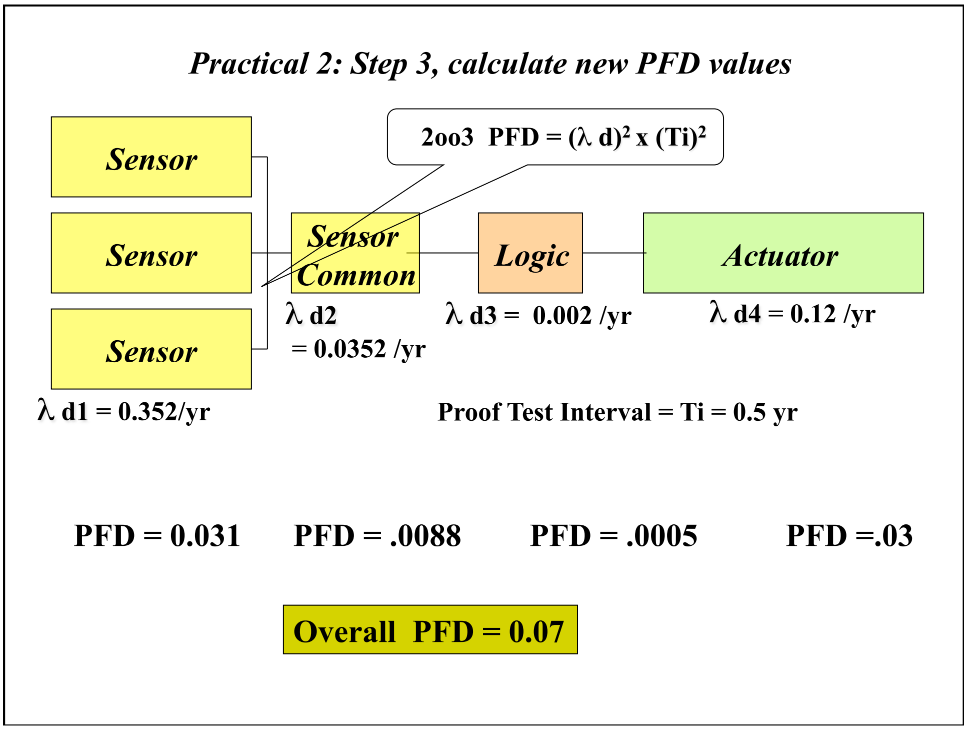
3/4/11


1oo1 Relay trip
Drench Tank
TSH
FO
Single Channel
High temperature
Trip
TT
TE
Reactor

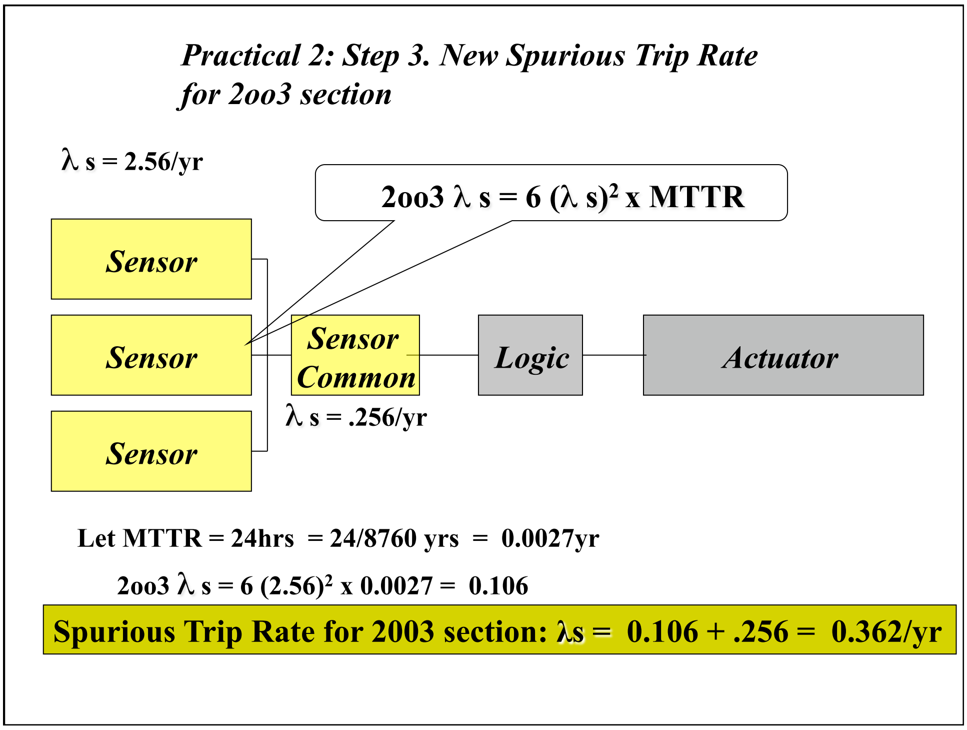

Spurious fault rate λ s
λ s = 1.5 + 0.5 + 0.01 + 0.5 + 0.05 + 0.05 + 0.01 + 0.04 + 0.4
TE
TT
Cab
TSH
1R
1R
Cab
Sov
Valve
λd = 0.2 + 0.05 + 0.00 + 0.1 + 0.002 +0.002 + 0.00 + 0.02 + 0.1
Dangerous fault rate λd
λ s = 2.56 /yr
λ s = 0.05 /yr
λ s = 0.45 /yr
Sensor
Logic
Actuator
λd = 0.352 /yr
PFD = .088
λd = 0.002 /yr
PFD = .0005
λd = 0.12 /yr
PFD =.03
Proof Test
Interval = 0.5 yr
Practical 6: Step 1
Single Channel: PFD = 0.118
Spurious Trip Rate: λ s = 3.06/yr


2oo3 Relay trip
TSH
TSH
TSH
Drench Tank
FO
TT
TT
TE
TE
TT
TE
2oo3 Input Voting
High temperature
Trip
Reactor

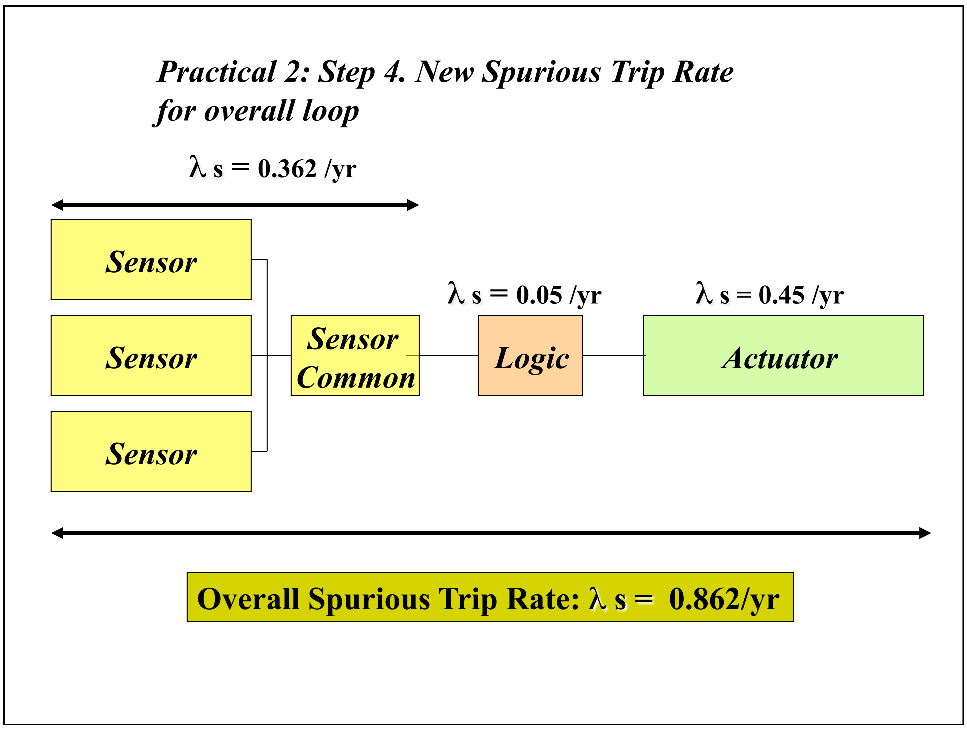

Practical 2: Step 2,
calculate new values for λs and λd when sensors
are changed to 2oo3
Sensor Common
Cause Factor = 10%
λs = 2.56 /yr
λ s = 10% x 2.56
0.256 /yr
λ s = 0.05 /yr
λ s = 0.45 /yr
Sensor
Sensor
Sensor
Sensor
Common
Logic
Actuator
λ d1
= 0.352 /yr
λ d2
= 10% x 0.352
= .0352/yr
λ d3
= 0.002 /yr
λ d4
= 0.12 /yr



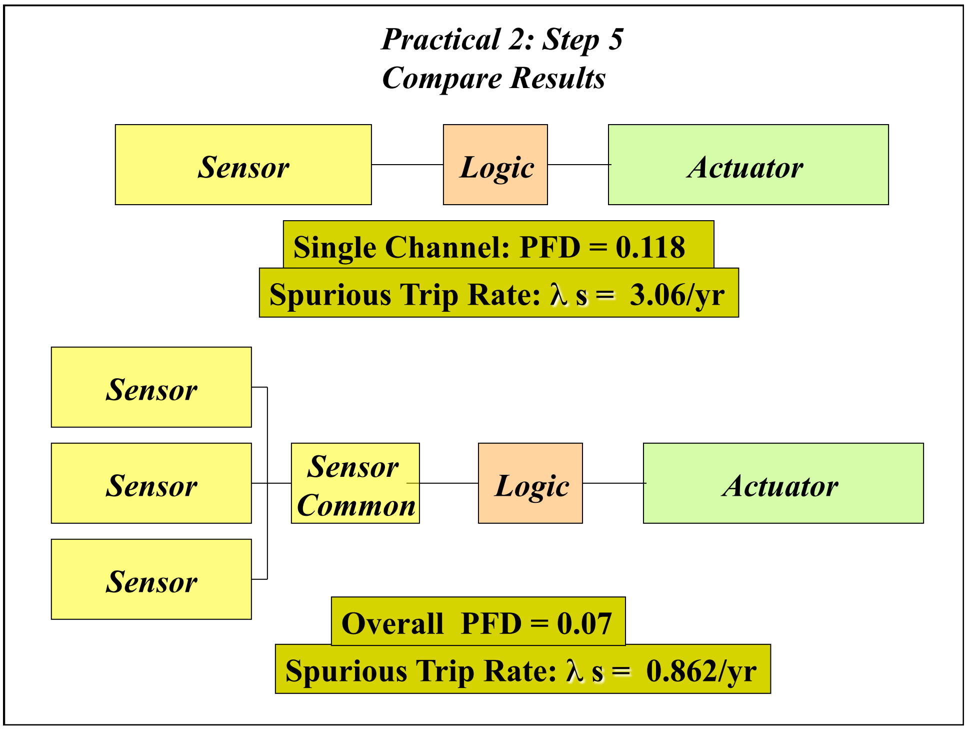
Practical 2: Step 3, calculate new PFD values
2oo3 PFD = (λ d)² x (Ti)²
Sensor
Sensor
Sensor
Sensor Common
Logic
Actuator
λ d2 = 0.0352 /yr
λ d3 = 0.002 /yr
λ d4 = 0.12 /yr
λ d1 = 0.352/yr
Proof Test Interval = Ti = 0.5 yr
PFD = 0.031
PFD = .0088
PFD = .0005
PFD =.03
Overall PFD = 0.07



Practical 2: Step 3. New Spurious Trip Rate for 2oo3 section
λ s = 2.56/yr
2oo3 λ s = 6 (λ s)² x MTTR
Sensor
Sensor
Sensor
Sensor Common
Logic
Actuator
λ s = .256/yr
Let MTTR = 24hrs = 24/8760 yrs = 0.0027yr
2oo3 λ s = 6 (2.56)² x 0.0027 = 0.106
Spurious Trip Rate for 2003 section: λs = 0.106 + .256 = 0.362/yr



Practical 2: Step 4. New Spurious Trip Rate for overall loop
λ s = 0.362 /yr
Sensor
Sensor
Sensor
Sensor Common
λ s = 0.05 /yr
Logic
λ s = 0.45 /yr
Actuator
Overall Spurious Trip Rate: λ s = 0.862/yr



Practical 2: Step 5
Compare Results
Sensor
Logic
Actuator
Single Channel: PFD = 0.118
Spurious Trip Rate: λ s = 3.06/yr
Sensor
Sensor
Sensor
Sensor Common
Logic
Actuator
Overall PFD = 0.07
Spurious Trip Rate: λ s = 0.862/yr

Exercise No: 3 - Determination of SIL by Risk Graph

This practical exercise requires participants to determine the required SIL of a proposed safety-instrumented system using the basic principles and risk graphs and calibration parameters for safety, environment and asset loss described in this module

The process is a reactor with a continuous feed of fuel and oxidant. Two flow control loops are operated under a ratio controller set by the operator to provide matching flows of fuel and oxidant to the reactor. An explosive mixture can occur within the reactor if the fuel flow becomes too high relative to the oxidant flow.

Possible causes are: Failures of the BPCS or an Operator error in manipulating the controls leading to sudden loss of oxidant feed.

A SIS is proposed with a separate set of flow meters connected to a flow ratio measuring function that is designed to trip the process to safe condition if the fuel flow exceeds the oxidant flow by a significant amount

The tag number for this function is FFSH- 03

Assume that the following information has been decided for the reactor.

The total frequency of the events leading to an explosive mixture is approximately once every ten years.

The consequence of the explosion has been determined to be a vessel rupture causing death or serious injury to 1 person

The occupancy in the exposed area is less than 10% of the time and is not related to the condition of the process.

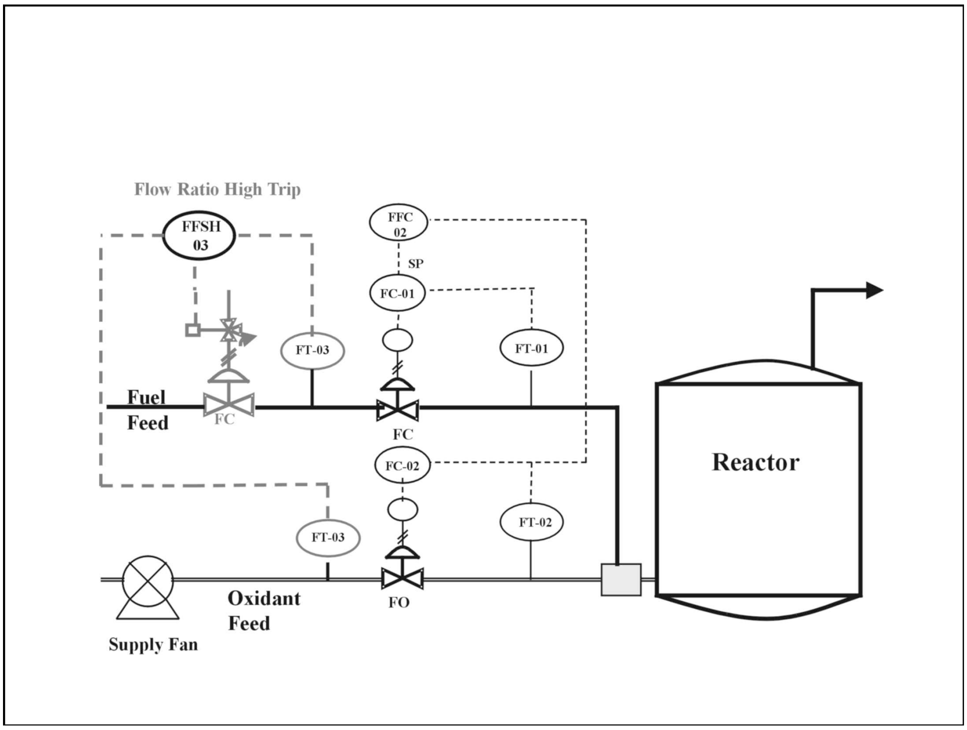
The onset of the event is likely to be to be fast with a worst-case time of 10 minutes between loss of oxidant and the possible explosion.

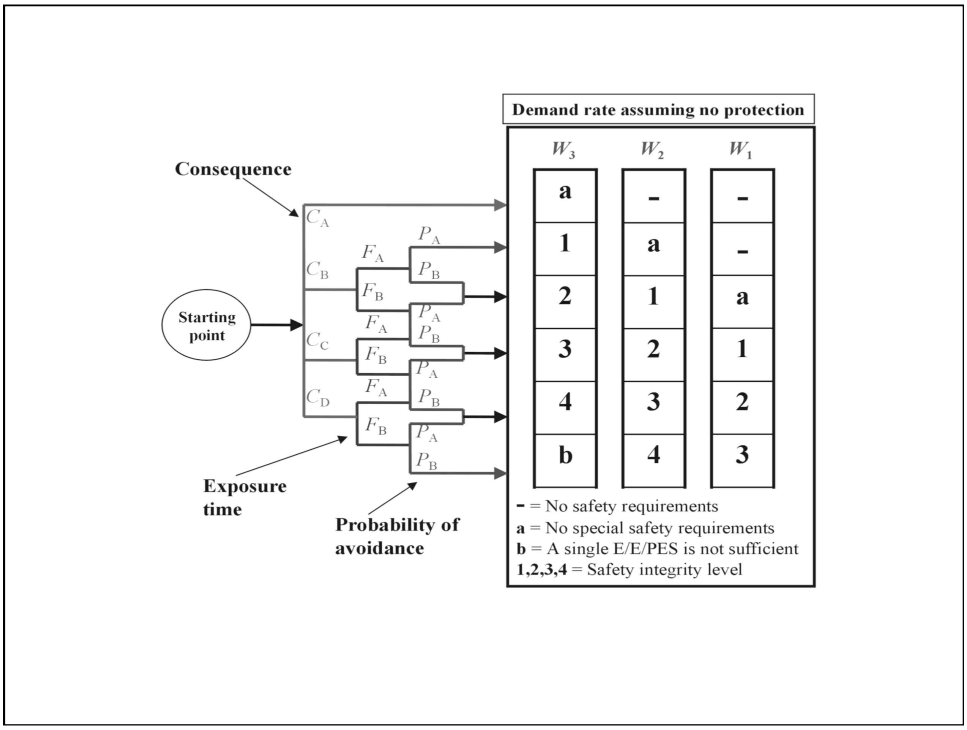
The material released from an explosion is not harmful to the environment.

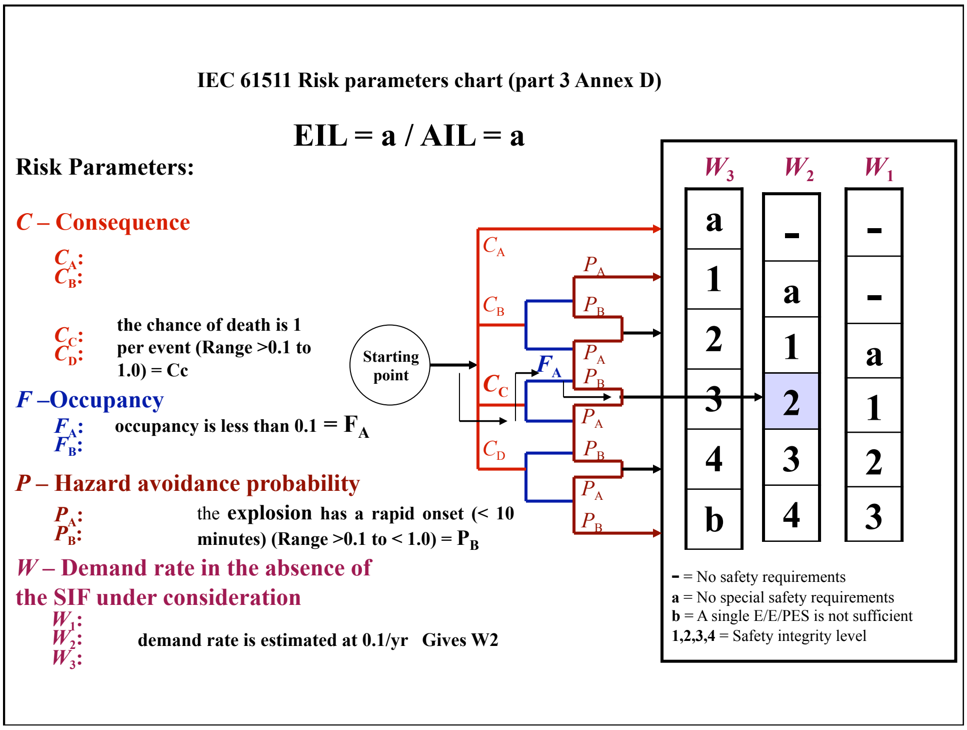
The reactor will cost in excess of £250, 000 to replace.

Determine the target SIL, EIL and AIL

Determine the overall target integrity for the SIF


Flow Ratio High Trip
FFSH 03
FFC 02
SP
FC-01
FT-03
FT-01
Fuel Feed
FC
FC
FC-02
FT-03
FT-02
Reactor
Oxidant Feed
FO
Supply Fan


Demand rate assuming no protection
W3
W2
W1
Consequence
Starting point
Exposure time
Probability of avoidance
a 1 2 3 4 b
- a 1 2 3 4
- - a 1 2 3
- = No safety requirements
a = No special safety requirements
b = A single E/E/PES is not sufficient
1,2,3,4 = Safety integrity level


IEC 61511 Risk parameters chart (part 3 Annex D)
EIL = a / AIL = a
Risk Parameters:
C – Consequence
C_A:
C_B:
C_C: the chance of death is 1 per event (Range >0.1 to 1.0) = Cc
C_D:
F –Occupancy
F_A: occupancy is less than 0.1 = F_A
F_B:
P – Hazard avoidance probability
P_A:
P_B: the explosion has a rapid onset (< 10 minutes) (Range >0.1 to < 1.0) = P_B
W – Demand rate in the absence of the SIF under consideration
W_1:
W_2: demand rate is estimated at 0.1/yr Gives W2
W_3:
Starting point
C_A
C_B
C_C
C_D
F_A
P_A
P_B
W_3
W_2
W_1
a 1 2 3 4 b
- a 1 2 3 4
- - a 1 2 3
- = No safety requirements
a = No special safety requirements
b = A single E/E/PES is not sufficient
1,2,3,4 = Safety integrity level

Exercise No: 4 - Determination of SIL by LOPA

This practical exercise requires participants to determine the required SIL of a proposed SIS using the basic principles and LOPA parameters described in this module

Liquid is transferred manually to a holding tank before delivery to the plant, the operator must stop the pump at 75% Tank Level.

A Tank Over pressurisation hazard has been identified by the HAZOP team, two causes have been identified:

- Operator fails to stop pump : 0.1 per year
- Level Control Failure: 0.1 per year

Determine the required target SIL for personnel safety of the High Pressure Vent SIF to Flare

ProSalus Limited

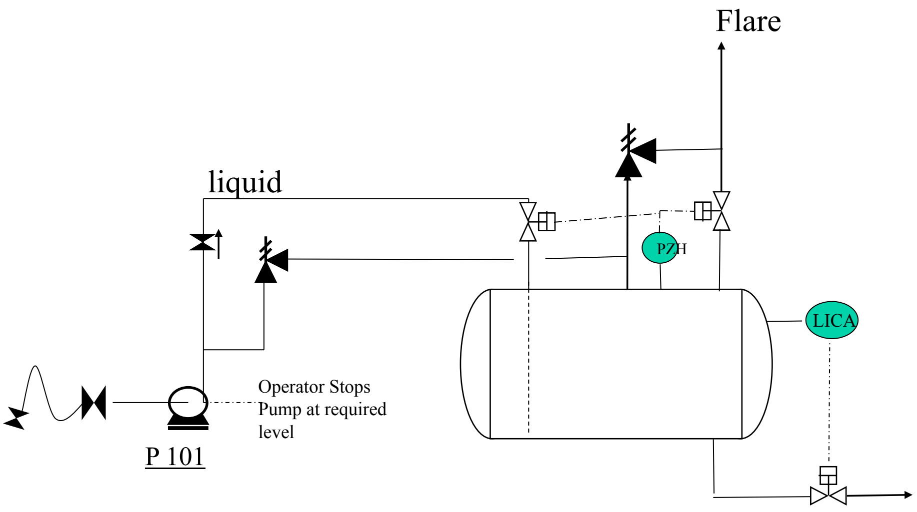
Exercise No: 4 - Determination of SIL by LOPA

The tolerable risk for the hazard is 1.0E-05

The Holding tank has a relief valve installed which is sized for full flow and vented to Flare

The process design is not considered to be fit for purpose

ProSalus Limited



ProSalus Limited

LOPA Worksheet

	1	Impact Event	Overpressure of Tank	
Likelihood are event/year and protection are PFD Average	2	Severity Level	S	S
	3	Initiating Cause	Operator Error	LC failure
	4	Initiation Likelihood	0.1	0.1
Protection & Mitigation Layers	5	General Design	1	1
		Control System	0.1	1
		Independent Alarm	1	1
	6	Additional Mitigation, Relief Valve	0.01	0.01
	7	Additional Mitigation, Closed Drain	1	1
	8	Intermediate Event Likelihood	1.0E-04	1.0E-03
	9	Total Mitigated Event Frequency	1.1E-03	
	10	PFDavg required	1.0E-05/1.1E-03 = 9.1E-03 (SIL2)	
	11	Tolerable Mitigated Event Likelihood	1.0E-05	
	11	Notes		